JURNAL RESPONSIVE
Teknik Informatika

Juni 2025 | Vol. 9 | No. 1
E-ISSN : 2614-7602
DOI: 10.36352/jr.v9i01.1178

ANALISIS TANTANGAN KEAMANAN JARINGAN IOT DAN STRATEGI MITIGASINYA

Maria Triani Mbejo*[1], Indra Sufian[2]
[1,2]Program Studi Teknik Informatika, Fakultas Sains dan Teknologi– Universitas Ibnu Sina, Batam
e-mail: *[1]231055201001@uis.ac.id [2]indra.sufian@uis.ac.id

Abstrak

Perkembangan *Internet of Things* semakin menunjukkan angka yang signifikan, istilah IoT sendiri pertama kali dicetus oleh Kevin Ashton, seorang ilmuwan computer yang saat itu bekerja di *Protector&Gambel*. Tanpa disadari IoT relah mengubah gaya hidup dan hubungan kita dengant eknologi menjadi hamper tidak bisa terlepaskan. Bersama dengan pertumbuhan yang pesat ini, berbagai tantangan keamanan juga tidak dapat terhindarkan diantaranya integritas data, resiko autentikasi dan enkripsi yang lemah, segmentasi jaringan yan gkurang memadai, serta pembaruan perangkat yang sering diabaikan. Dari beberapa tantangan ini menimbulkan beberapa jenis serangan seperi *Distributed Denial of Service* (DDoS) yang akan membajiri lalu lintas komunikasi, informasi dan jaringan pengguna dengan permintaan berlebihan. Menurut data dari, Pada quartal pertama tahun ini saja, peningkatan serangan DDoS padaperangkat mencapai 20, 5 juta serangan. Jenis serangan lain pada perangkat IoT adalah *Man in the Middle Attack* (MitM) dimana, peretas menyusup di tengah tengah komunikasi dua server, atau menurut, serangan MitM terjadi saat pelaku peretasan berada di jaringan yang sama dengan perangkat yang akan diserang. Adapun Teknik pencegahan yang dapat diterapkan adalah menggunakan *Firewall* dan Sistem Deteksi Intrusi, menggunakan enkripsi *end to end*, mengaktifkan autentikasi 2FA, membatasi lalu lintas dan Rate limiting, menggunakan jaringan tersegmentasi hingga pembaruan *firmware* dan perangkan lunak. Kemanan akan perangkat IoT bukan lagi menjadi masalah sepeleh melainkan untuk selalu diperhatikan dan ditangani dengan baik.

Kata kunci IoT, DDoS, MitM, *Firewall, Firmware*

Abstract

The development of the Internet of Things is increasingly showing significant numbers, the term IoT itself was first coined by Kevin Ashton, a computer scientist who was then working at Protector & Gamble. Unwittingly, IoT has changed our lifestyle and relationship with technology to be almost inseparable. Along with this rapid growth, various security challenges are also unavoidable, including data integrity, weak authentication and encryption risks, inadequate network segmentation, and often ignored device updates. From some of these challenges, several types of attacks arise, such as Distributed Denial of Service (DDoS) which will flood communication traffic, information and user networks with excessive requests. According to data from, In the first quarter of this year alone, the increase in DDoS attacks on devices reached 20.5 million attacks. Another type of attack on IoT devices is the Man in the Middle Attack (MitM) where hackers infiltrate the middle of two server communications, or according to, MitM attacks occur when the hacker is on the same network as the device to be attacked. The prevention techniques that can be applied are using Firewalls and Intrusion Detection Systems, using end-to-end encryption, activating 2FA authentication, limiting traffic

and Rate limiting, using segmented networks to firmware and software updates. Security of IoT devices is no longer a trivial matter but must always be considered and handled properly.

Keywords—IoT, DDoS, MitM

PENDAHULUAN

Belakangan ini, perkembangan *Internet of Things* (IoT) makin menunjukan angka yang signinfikan, membuatnya menjadi hal *basic* di kalangan penggunanya, "IoT menawarkan berbagai macam layanan yang membuatnya lebih cepat untuk berkembang, dengan dampak yang besar pada kehidupan social dan lingkungan bisnis." [1]. Dibalik keberahasilan ini tentu tidak luput dari kesalahan atau eror keamanan data dan jaringan yang kurang terjamin. Masalah keamanan sudah menjadi tantangan umum bukan hanya dalam dunia IoT.

Referensi [2] menyebutkan Istilah "*Internet of Things*" Pertama kali dikenal pada tahun 1999 yang dicetuskan oleh Kevin Ashton, seorang ilmuwan computer yang saat itu bekerja di Procter&Gamble. Ia menyebutkan istilah ini dalam presentasinya kengenai konsep pengguanaan RFID untuk melacak produk dalam rantai pasokan. "Banyak peneliti yang mendefinisikan IoT menggunakan istilah yang berbeda merujuk pada IoT sebagai serangkaian perangkat yang saling terhubung dan dapat saling berkomunikasi" [3]. juga mendefinisakan istilah sederhana dari IoT yang adalah jaringan perangkat yang menggunakan internet dengan media transmisi kabel maupun nirkabel untuk saling berkomuniasi menggunkan komunikasi *Machine to machine* (M2M).

Internet of Things secara tidak langsung telah mengubah gaya hidup hubungan kita dengan teknologi yang dulunya tidak begitu intens menjadi suatu hibunganyang hamper tidak bisa lepas dari keseharian kita. Hal ini karena IoT telah memungkinkan semua perangkat elektronik disekitar kita menjadi bagian dari satu jaringan yang terintegrasi. IoT telah berpindah dari ruang kerja ke rumah kita melalui perangkat-perangkat pintar yang dapat mempermudah pekerjaan rumah. Contoh paling sederhana ialah **Smart home** menyediakan konsep di mana semua peralatan rumah tangga dapat dikontrol dari satu pusat, sering kali melalui aplikasi di *smartphone*, *tablet*, atau komputer. Dengan sistem ini, semua peralatan listrik dan elektronik di rumah dapat dikendalikan secara terpusat, baik dari jarak dekat maupun jauh [4]. Perangkat dalam *smart home* misalnya alat memasak cukup tidak memungkinkan untuk diretas karena peretas tidak bisa melakukan banyak hal dengan peralatan dapur seperti ini.

Selain *Smart home* penerapan IoT juga mencakup fitur-fitur pengendalian jarak jauh, pemrosesan data dengan sensor yang canggih yg terpasang pada peralatan fasilitas umum, misalnya kamera atau CCTV jalan dengan deteksi Tindakan kriminal untuk kebutuhan keamanan. Dalam sektor Pendidikan fitur ini dipasang untuk pemrosesan data kehadiran serta pelacakan siswa untuk membuat sekolah lebih aman. Dalam sektor industri, fitur sensor juga diterapkan untuk memproses data karyawan di sebuah perusahaan mnjadikannya lebih efisien serta memberikan kontrol Kesehatan dan keselamatan pekerjanya. Selain fitur sensor, menurut [1] dalam sektor Pendidikan juga telah mulai membuat sistem Pendidikan konvensional lebih otomatis. Misalnya kelas pintar yang interaktif dapat membantu siswa belajar dan berpartisipasi lebih banyak.

Seiring dengan perkembang yg signifikan, resiko peretasan dan phising menjadi tidak terelakkan. Internet telah membuka pintu bagi peretas untuk mengeksploitasi kelemahan, dengan begitu dalam penelitian ini membahas tantangan keamanan jaringan pada IoT serta metode pencegahan yang dapat dilakukan.

TINJAUAN LITERATUR

1.1 Pengertian IoT

Internet of Things (IoT) merupakan suatu sistem yang terdiri dari perangkat, objek, dan mesin yang saling terhubung dan memiliki kemampuan untuk mentransfer data melalui jaringan internet [5]. Istilah "Things" dalam konteks IoT merujuk pada berbagai jenis perangkat yang dapat terhubung ke internet, seperti smartphone, mesin cuci, kendaraan, kamera keamanan, hingga alat kesehatan [6]. Menurut penelitian oleh Informatika Universitas Janabadra [5], setiap perangkat dalam ekosistem IoT mampu saling berkomunikasi, mengumpulkan data, menganalisis informasi yang diperoleh, dan bahkan melakukan tindakan secara otomatis berdasarkan data tersebut tanpa campur tangan manusia.

1.2 Penelitian Terdahulu

Penelitian ini menggunakan pendekatan studi literatur dengan mengkaji sejumlah jurnal dan laporan penelitian terdahulu yang membahas secara spesifik berbagai tantangan keamanan dalam jaringan Internet of Things (IoT). Salah satu penelitian yang dirujuk adalah oleh Mohit dan Rakesh [1], yang mengidentifikasi bahwa salah satu tantangan signifikan dalam ekosistem IoT adalah pengelolaan pembaruan perangkat. Ditegaskan bahwa jutaan perangkat IoT membutuhkan pembaruan rutin untuk menjaga keamanan, namun tidak semua perangkat mendukung pembaruan over-the-air (OTA). Kondisi ini menuntut pengguna untuk melakukan pembaruan secara manual, yang berpotensi diabaikan dan menjadi celah keamanan.

Selain itu, berdasarkan kajian yang dilakukan oleh Makhdoom et al. [7], ancaman serius dalam sistem IoT terletak pada integritas perangkat lunak, termasuk sistem operasi, aplikasi, dan konfigurasi perangkat. Ancaman terhadap integritas ini dapat membuka potensi akses tidak sah dan manipulasi data, yang membahayakan privasi serta kestabilan jaringan IoT.

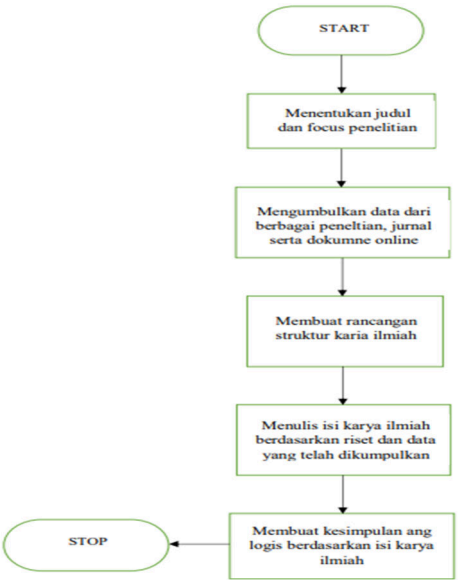
Sementara itu, kajian oleh W. Najib et al. [8] meninjau model arsitektur jaringan IoT tujuh lapis dan menekankan bahwa ancaman keamanan dapat terjadi terutama pada bagian edge side, yang mencakup lapisan Edge Nodes, komunikasi, dan komputasi tepi (Edge Computing). Lapisan-lapisan ini sangat rentan terhadap serangan karena menjadi titik awal interaksi antara perangkat IoT dengan jaringan dan sistem cloud yang lebih besar.

1.3 Sistem Kemanan Perangkat IoT

Keamanan perangkat *Internet of Things* (IoT) merupakan bagian integral dari strategi keamanan siber yang bertujuan untuk melindungi perangkat-perangkat terhubung serta jaringan yang digunakan dari berbagai ancaman siber. Menurut Fortinet [9], keamanan IoT mencakup upaya untuk mengamankan perangkat keras, perangkat lunak, serta komunikasi data yang berlangsung antarperangkat. Perangkat IoT sering kali terhubung dalam jaringan yang memiliki tingkat kerentanan tinggi karena keterbatasan sumber daya, kurangnya standar keamanan yang konsisten, dan kompleksitas arsitektur sistem. Oleh karena itu, strategi keamanan IoT perlu mencakup mekanisme seperti autentikasi yang kuat, enkripsi data, segmentasi jaringan, serta pemantauan lalu lintas jaringan secara terus-menerus untuk mendeteksi dan mencegah potensi serangan sebelum berdampak lebih luas.

METODE PENELITIAN

Penelitian bersifat kualitatif yaitu dengan menguraikan data dan sumber Pustaka dan literatur dari penelitian terdahulu dari jurnal, laporan, buku hingga publikasi ilmiah serta dokumen *online* lainnya yang dijadikan dasar dari proses penulisan karya ilmiah ini. Berikut *Flowchart* dari alur penelitian ilmiah ini.



Gambar 1. Alur Penelitian

Teknik analisis yang dilakukan adalah analisis Deskriptif Yaitu dengan menggambarkan kondisi kemanan IoT saat ini berdasarkan data dan literatur serta menyajikan fakta terkait ancaman umum seperti dan DDoS, *malware* dan serangan *Man-in-the-Middle*.

HASIL DAN PEMBAHASAN

1.4 Tantangan Keamanan dalam Jaringan IoT

Keamanan dalam jaringan IoT adalah perlindungan perangkat *Internet of Things* dari serangan. Perangkat IoT ada dimana-mana dalam kehidupan kita akhir-akhir ini. Menurut data dari Statista, akan ada 75,44 miliar perangkat IoT akan terpasang pada tahun 2025. Ini merupakan peningkatan yang tajam dari tahun tahun sebelumnya. Perangkat IoT sebagian besar terhubung ke internet atau perangkat *gateway* melalui media komunikasi nirkabel yang lebih lambat dan kurang aman seperti 802.15.4, 802.11a/b/g/n/p, LoRa, ZigBee, NBIoT, dan SigFox. Akibatnya, sistem IoT rentan terhadap kebocoran data dan masalah privasi lainnya. [7]. Beberapa tantangan dan ancaman serangan keamanan siber tidak dapat terhindarkan. Berikut ini beberapa tantangan utama keamanan IoT dari referensi:

a. Integritas Data
   Semakin tahun semakin banyak perangkat berada dibawah naungan ekosistem yang saling terhubung melalui IoT. Referensi [1] menyatakan Memanipulasi satu titik data saja akan menghasilkan berdampak ke seluruh data yang saling bertukar informasi dan dibagikan bolak-balik dari sensor ke server utama.

b. Resiko Autentikasi dan Enkripsi yang Lemah
   Kurangnya Enkripsi dan auntentikasi juga dapat membuat keamanan perangkat IoT menjadi terancam. Dengan enkripsi yang memadai, dapat mengamankan jaringan yang saling terhubung agar informasi sensitif seperti data pelanggan, transaksi keuangan, dan komunikasi internal dapat terlindungi dari akses tidak sah. “Enkripsi melibatkan pengodean data sehingga hanya pihak yang berwenang yang dapat mengaksesnya. “ [10]. Sehingga perangkat yang tidak dienkripsi dengan baik dapat disadap oleh pihak yang tidak berwenang. Data yang dikirim bisa diubah atau dicuri, yang berisiko menyebabkan kebocoran informasi

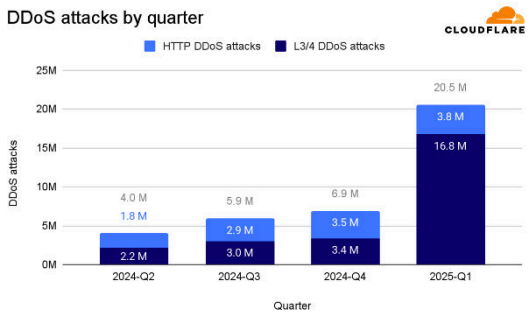
sensitif. “Enkripsi juga memerlukan daya pemrosesan. Semakin baik dan kuat enkripsi, akan semakin banyak juga daya komputasi yang dibutuhkan untuk menjalankannya.”[11].
Keamanan perangkat IoT tidak hanya bergantung pada enkripsi tetapi juga pada autentikasi. Autentikasi yang yang lemah misalnya sandi yang dibuat default atau PIN yang sederhana dapat memudahkan peretas untuk memecahkannya dan mendapat akses bebas ke perangkat IoT kita sehingga terjadi pencurian data, kontrol perangkat yang tidak sah serta potensi intrusi jaringan yang lebih besar lainnya. Perangkat yang tidak terlindungi juga berpotensi dijadikan bagian dari botnet, yaitu jaringan perangkat yang diretas untuk melancarkan serangan siber, seperti serangan *Distributed Denial of Service* (DDoS).

c. Segmentasi Jaringan Kurang Memadai
Segmentasi jaringan yang buruk sering kali memungkinkan penerang bergerak secara lateral setelah membobol satu sistem. Tanpa pemidahan antara lingkunagan IT, OT dan IoT, perangkat IoT yang disusupi seperti *thermostat* pintar, dapat menyebabkan akses ke sistem kontrol industri atau data sensitif[12].

d. Pembaruan
Tidak semua perangkat mendukung lebih dari pembaruan otomotis oleh karenannya dibutuhkan pembaruan secara manual. Investasi keamanan dalam pengaman infrastruktur dan jaringan harus menjadi prioritas utama. IoT melibatkan penggunaan jutaan titik data dan setiap titik harus diamankan[1].

1.5 Jenis Serangan Perangkat IoT

a. Serangan *Distributed Denial of Service* (DDoS)
Menurut [13], Serangan DDOS merupakan jenis serangan jaringan IoT ysng paling umum dan menjadi salah satu masalh paling serius yang dihadapi oleh konsultan TI dan professional kemanan. DDoS *Attack* adalah serangan yang menggaggu jaringan sumber daya perangkat dengan membanjiri lalu lintas komunikasi dengan permintaan yang bertubi-tubi yang membuat server mengalami *lag* dan kebingungan untuk melanjutkan interaksi dengan server lain atau user. Menurut [13], serangan ini cukup sulit untuk dicegah dan dideteksi karena menggunakan lokasi serta perangkat yang berbeda untu kmelakukan serangan.
Seiring dengan perkembangan dan penggunaan IoT yang pesat, serangan DDoS juga ikut meningkat pesat hingga quarter pertama tahun ini. Berdasarkan data dari [14], peningkatan serangan DDoS pada tahun 2025 saja mencapai 20,5 juta serangan.



Gambar 2. Diagram Peningkatan serangan DDoS
Sumber: *Cloudflare*

b. Serangan *Man in the Middle*
Serangan MitM adalah serangan yang terdiri dari korban (dua pengguna) yang saling berkomunikasi serta penyerang yang merupakan pihak ketiga dari jaringan jomunikasi tadi. Penyerang melakukan penyusupan diantara dua pengguna tadi dan pengguna tidak menyadari bahwa ada pihak ketiga diantara komunikasi mereka. [15]. [16] mendefinisikan

serangan MitM terjadi saat pelaku peretasan berada di jaringan yang sama dengan perangkat yang akan diserang. Referensi [15] juga menyatakan MitM ini dapat di arahkan ke berbagai jalur komunikasi yang terdiri dari GSM, *Wi-Fi*, UMTS dan Bluetooth agar data mengalir di anatar titik-titik akhir serta menginfeksi integritas data. Tujuan dari serangan ini adalah untuk mencuri data dan informasi pribadi yang sedang ditransmisikan untuk disalahgunakan. MitM ini dikategorikan jenis serangan pasif karena hanya menyadap informasi dan komunukasi korbannya.

a. Teknik Pencegahan

Meninjau dari ancaman keamanan yang diuraikan diatas, beberapa Langkah-langkah pencegahan dapat dilakukan untuk melindungi sistem dari peretasan.

1. Menggunakan *Firewall* dan Sistem Deteksi Intrusi (IDS)
   Firewall dapat memblokir lalu lintas mencurigakan, sementara IDS membantu mendeteksi pola serangan sebelum terjadi. Teknik ini dapat digunakakn untuk melindungi perangkat dri serangan DDoS [17].
2. Menggunakan Enkripsi *End-to-End*
   Memastikan komunikasi antar perangkat IoT menggunakan protokol seperti TLS atau VPN agar terhindar dari seranan MitM
3. Mengaktifkan Autentikasi Dua Faktor (2FA)
   Menambahkan lapisan ekstra untuk akses ke perangakt IoT [18]
4. Membatasi Lalu Lintas dan *Rate Limiting*
   Mengatur batas permintaan yang dapat diterima oleh perangkat IoT untuk menghindari banjir lalu lintas[19] yang di sebabkan oleh DDoS.
5. Menggunakan Jaringan Tersegmentasi
   Memisahkan perangakat IoT dari Jaringan utama untuk mengurangi dampak serangan[17].
6. Pembaruan *Firmware* dan Perangkat Lunak
   Pastikan perangkat IoT selalu menggunakan versi terbaru untuk menutup celah peretasan[19].

KESIMPULAN

Seiring dengan pesatnya pertumbuhan teknologi era ini, inovasi dan temuan baru perangkat IoT juga ikut berkembang dan menjadi bagian yang hampir tidak bisa dipisahkan dari kehidupan kita sehari-hari, resikoa ancaman keamanan jaringan perangkat IoT juga ikut meningkat sehingga perlu dinilai dan dikembangkan Teknik pencegahannya. Terkadang beberapa perangkat IoT tidak terlalu aman dan mungkin vendornya tidak melakukan pembaruan perangkat lunak *firmware* karena tidak adanya dukungan pengembangan yang membuat perangkat yg digunakan menjadi rentan untuk diretas. Beberapa Teknik pencegahan diatas dapat diterapkan untuk mengamankan perangkat.

Penyebab utama daripada resiko ancaman kemanan jaringan adalah karena setiap perangkat ini terhubung ke internet saat digunakan yang dimana dapat memungkinkan peretas untuk menyusup dan meretas perangkat tersebut dan menggunakannya untuk mengakses jaringan perangkat kita. Salah satu Teknik pencegahan yang paling sederhana untuk melindungi jaringan komunikasi perangkat kita, adalah memisahkan perangkat IoT yang digunakan dari jaringan utama untuk mengurangi dampak serangan.

DAFTAR PUSTAKA

[1] Mohit S., Rakesh K. S. (2019). "*Internet of Things (IoT) Applications and Security Challenges: A Review*". *Special Issue,* vol 7, Edisi 12, pp. 1, 5-7.

[2] Netmonk. (June 13 2019). Internet of Things (IoT). Chap. 1.

[3] N. N. Thilakarthne, M. S. Abu Bakar, H. E. Abas, H. Yassin, (2025). "*Internet of things enabled smart agriculture: Current status, latest advancements, challenges and countermeasure*."

[4] Rita P. S., (2024, August). "Penerapan IoT dalam Smart Home dan Manfaatnya. *Cloud Computing* Indonesia." Chap. 4. Diakses tanggal 15 Mei 2025 dari https://www.cloudcomputing.id/pengetahuan-dasar/penerapan-iot-smar-thome#:~:text=Apa%20itu%20Smart%20Home?,dari%20jarak%20dekat%20maupun%20jauh

[5] Informatika Universitas Janabadra. n.d, "Konsep Dasar Internet of Thins: Mengenal Jaringan Terhubung dan Membawa Perubahan." Chap. 1. Diakses tanggal 15 Mei 2025 dari https://informatika.janabadra.ac.id/konsep-dasar-internet-of-things-iot-mengenal-jaringan-terhubung-yang-membawa-perubahan/#:~:text=Internet%20of%20Things%20(IoT)%20adalah,tanpa%20perlu%20campur%20tangan%20manusia.

[6] I. Prasetyo, (October 30 2024).Telkom University." Apa itu Internet of Things? Pengertian, Cara Kerja, dan Contohnya." Chap. 1. Diakses tanggal 15 Mei 2025 dari https://docif.telkomuniversity.ac.id/apa-itu-iot/

[7] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of Threats to the Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, p. 6, Secondquarter 2019."

[8] W. Najib, S. Sulistyo, Widyawan. Dalam Jurnal Nasional Teknik Elektro dan Teknologi Informasi. "Tinjauan Ancaman dan Solusi Kemanan pada Teknologi *Internet of Things".* Vol. 9 No. 4, November 2020, pp. 377, 378.

[9] Fortinet. n.d, "Apa itu Keamanan IoT? Tantangan dan Persyaratan". Chap. 1.

[10] *Nexus In groupe.* (28 March, 2024). *What Are The Security Challenges of IoT?*. Chap. 6, diakses tanggal 29 Mei 2025 dari https://www.nexusgroup.com/what-are-the-security-challenges-of-iot/

[11] David G., (n.d). IoT security: "Why you need ro encrypt your data." Verizon. Chap. 3. Diakses tanggal 29 Mei 2025 dari https://www-verizon-com.translate.goog/business/resources/articles/s/iot-security-why-you-need-to-encrypt-your-data

[12] T. Olaes. Balbix. "Top IT, and IoT Security Challenges and Best Practices." updated: May 1 2025. Chap 5. Diakses tanggal 30 Mei 2025 dari https://www.balbix.com/insights/addressing-iot-security-challenges/

[13] P. Kumari, A. K. Jain., April 2023. *Journal Computer&Security*, vol. 127., "*A comprehensive study of DDoS attacks over IoT network and their countermeasurs".* P.1. DOI: https://doi.org/10.1016/j.cose.2023.103096

[14] O. Yoachimik, J. Pacheco. April 27 2025. *Cloudflare.* "*Targeted by 20.5 million DDoS attacks, up 358% year-over-year: Cloudflare's 2025 Q1 DDoS Threat Report*". Chap. 2

[15] D. Javeed, U. M. Badamasi, C. O. Ndubuisi, F. Soomro, M. Asif. "*Man in the Middle Attacks: Analysis, Motivation and Prevention.*" VOL. 8, No. 7, July 2020, 52-58, p. 1, DOI: 10.13140/RG.2.2.22752.81928

[16] Serhat C., Nesibe Y., Semih C. December 2023. "*MitM Attacks and IoT Security: A Case Study on MQTI"*. Vol. 3, No. 2, pp. 99-106.

[17] Mei. Nusabot. July 4 2024. "Mengidentifikasi dan Mencegah Serangan DDoS pada Perangkat IoT". Chap. 3. Diakses tanggal 31 Mei 2025 dari https://nusabot.id/blog/mengidentifikasi-dan-mencegah-serangan-ddos-pada-perangkat-iot/

[18] K. Sutisnawinata. ASDF.ID. November 14 2023. "*Man in the Middle Attack*: Arti, Cara Kerja, Pencegahan" chap. 6. Diakses tanggal 31 Mei 2025 dari https://www.asdf.id/man-in-the-middle-attack-adalah/

[19] Azura Team. Azura Labs. October 21 2024, "Mendeteksi dan Mencegah Serangan DDoS pada Jaringan IoT", chap. 4, diakses tanggal 31 Mei 2025 dari https://azuralabs.id/blog-security-testing/mendeteksi-dan-mencegah-serangan-ddos-pada-jaringan-iot